

5 The rights information associated with audio files is generally stored as individual records in a content rights file on the file system of the target storage medium in the playback device (105, 110). The records in the content rights file include information such as how many times an audio file has been played or can be played, whether there is any absolute or relative expiration time associated with the audio file, and so on. Most conventional playback devices store the audio files in a file system that has a publicly documented command set. The CRM must therefore employ cryptographic means to ensure that the rights data associated with the audio files is not tampered with. Forms of tampering include file creation, deletion and renaming, and file content modification. To resist tampering, the file name of the content rights file is computed by hashing the device ID and the storage medium ID. The resulting hashed file name is stored in the secure storage area of the playback device (105, 110), where it can only be accessed by the device firmware and not by any users.

10 A process for transferring audio files with associated expiration information from the content server (160) to a particular playback device (105, 110) will now be described. It is assumed that a communication module for a playback device is connected to the communication network and that a user and the communication module for the playback device have been identified to the content server. The user who issues the request for having the files transferred to his or her playback device can also have registered himself or herself and the playback device, or has connected the playback device to the network, so that the corresponding user information and device information exist in the user database and device database, respectively.

15 As shown in FIG. 2, a process (200) for transferring audio files with expiration information starts with receiving a request from a communication module (120, 125) associated with a particular playback device (105, 110) of audio files to be transferred from the content server (160) to the communication module (120, 125) that is associated with the particular playback device (105, 110) (step 205). The request has been generated in response to a user initiated event, such as a user having selected files to be transferred from a conventional online store to his or her playback device for purchase, for rental, or for promotional purposes. Alternatively, the request can have originated at the content server (160), for example, if the user has selected a monthly subscription for a certain type of audio

files and the server has determined that it is time to deliver the next month's audio files to the user's playback device.

After the request has been received, the content server (160) obtains information about the device capability (step 210). This information can be obtained from a database in which the information has been previously stored, or from the communication module (120, 125) associated with the particular device (105, 110). The device capability information includes both physical information, such as what types of files the playback device (105, 110) can play, the available space on the playback device (105, 110), serial number, manufacturer, model, and so on, and information about what rights are associated with the playback device (105, 110) or with the user account associated with the playback device. Two users can, for example, have the same type of playback device (105, 110) but have different rights associated with their accounts, so that the first user can play files and transfer them to other playback devices (105, 110), while the second user only can play the files on the particular playback device (105, 110).

The content server (160) verifies the rights associated with the selected audio files, including the expiration rules for the audio files, against the obtained device capability (step 215). The rights associated with audio files are imposed by the audio file provider, and can include, for example, unlimited playback during a certain time period, free playback a certain number of times, playback a certain number of times within a given time period, and so on. The content server (160) then formats the selected audio files for the playback device (105, 110) and adds the rights including the expiration information to the audio files (step 220).

Alternatively, the content server can generate a license that controls what operations a user can perform on the audio files after they have been transferred to his or her playback device. The license can further include the expiration limitations, and is sent separately to the communication module. The license information with the content expiration information is stored separately at the user's playback device rather than being added to the audio files by the server at the remote side.

The audio files can additionally have other associated rights that control to what devices they may be transferred. For example, a file "Symphony No. 5" can have associated rights saying that it may only be transferred to devices that can time out content using dates and not play counts and that do not have more than 128 MB of total memory. There can also

be associated rights that relate to a user account rather than to device capabilities. For example a file "Symphony No. 2" can have associated rights saying that it can only be transferred to a device that is registered with a user account for which a premium subscription service has been selected. If the audio files have rights of this type associated, then the process checks these rights as well during the verification step.

The formatting of audio files for a particular playback device is described in U.S. patent application 09/894,846. The audio files are formatted so that they can only be played on the particular device or on a particular type of device. This can be done, for example, by using the serial number of the device when formatting the audio files. In an alternative implementation, the device can use a different ID such as a randomly generated 128 bit number implanted at the time a manufacturing, as the unique ID. A smaller, non-random serial number can be used for other purposes, such as customer service and repair and sales information tracking. In the case of a personal computer using a Windows Media Digital Rights Manager (WMDRM), the unique number can be obtained by prompting the WMDRM to generate a number. The WMDRM then generates a so called challenge number that is unique to that computer different every time it is generated. This number can be used as a unique identifier.

After the content server (160) has formatted the audio files, the audio files are transferred to the communication module (120, 125) for the particular playback device (105, 110) (step 225). The communication module (120, 125) stores the audio files either on the playback device (105, 110) or at an intermediary storage location, from which they are later transferred to the playback device (105, 110). The communication module can additionally perform content rights management functions on the audio files if the server sends content rights management commands.

After the files have been transferred to the playback device (105, 110), the process checks whether the user wishes to refresh the expiration information for any existing audio files on the playback device (105, 110) (step 230). If the user wishes to refresh rights associated with existing audio files, for example, if one or more of the files have expired, the process continues with refreshing the associated rights for the audio files (step 235), which will be further explained with reference to FIG. 4. If the user does not wish to refresh the rights, the process ends.